Exigences spécifiques pour les essais en vue de l'évaluation de la cybersécurité des produits TIC dans le cadre du schéma de certification européen EUCC (2024/482)

LAB REF 34 - Révision 00

SOMMAIRE

1. OBJET

Le présent document a pour objet de définir les exigences techniques et organisationnelles à satisfaire dans le cadre de l'accréditation des organismes en charge de l'évaluation de la cybersécurité des produits TIC conformément au schéma de certification EUCC.

Le cadre réglementaire pour cette accréditation est défini par le Règlement (UE) 2019/881 « Cybersecurity Act » et le Règlement d'exécution (UE) 2024/482 « EUCC ».

Ces dispositions sont mises en place conformément :

- aux obligations imposées par le schéma européen EUCC,
- à la norme NF EN ISO/IEC 17025 qui définit les exigences générales concernant la compétence des laboratoires d'essais et d'étalonnages, complétée notamment par la spécification technique ISO/IEC TS 23532-1 et le document Cofrac LAB REF 02.

Ce document ne se substitue pas à la réglementation, ni à la norme NF EN ISO/IEC 17025, ni aux documents Cofrac associés. Un défaut de prise en compte de ces exigences peut faire l'objet d'un écart, dont la criticité est appréciée conformément aux dispositions du Règlement d'accréditation LAB REF 05.

Le présent document couvre les familles ASE, APE, ACE, ACO, ADV, ALC, AGD, ATE et les composants AVA.VAN.1 et AVA.VAN.2[1] dans la série de normes ISO IEC 15408 (Critères Communs).

2. REFERENCES ET DEFINITIONS

2.1. Références

Les exigences de ce document s'appliquent en complément de celles des documents cités ci-après dans les § 2.1.1, 2.1.2 et 2.1.3. Il appartient à l'organisme accrédité ou candidat à l'accréditation de se tenir à jour des textes régissant les domaines concernés tant sur le plan technique que réglementaire.

Le § 2.1.4. liste des guides et normes techniques d'application recommandée.

2.1.1. Documents Cofrac et EA

- LAB REF 02 : Exigences pour l'accréditation des laboratoires selon la norme NF EN ISO/IEC 17025 : 2017 ;
- LAB REF 05 : Règlement d'accréditation ;
- LAB REF 08 : Expression et évaluation des portées d'accréditation ;
- GEN REF 11 : Règles générales pour la référence à l'accréditation et aux accords de reconnaissance internationaux ;
- LAB INF 34 : Nomenclature et expression des lignes de portées d'accréditation pour les essais en vue de l'évaluation de la cybersécurité des produits TIC dans le cadre du schéma de certification européen EUCC ;
- EA-2/20 G : 2020 Consultancy, and the Independence of Conformity Assessment Bodies.

[1] Les compétences techniques spécifiques pour l'évaluation de la robustesse des technologies mises en œuvre selon les composants AVA_VAN.3 à AVA_VAN.5 sont évaluées par l'ANSSI dans le cadre de l'autorisation du CESTI.

2.1.2. Normes et documents techniques

- NF EN ISO/IEC 17025 : Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais ;
- ISO/IEC TS 23532-1 : Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences des laboratoires d'essais et d'évaluation de la sécurité TI — Partie 1 : Évaluation pour l'ISO/IEC 15408 ;
- ISO/IEC 18045 : Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité ;
- ISO/IEC 15408 -1 à -5 : Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information ;
- Critères Communs : Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI, disponible sur commoncriteriaportal.org ;
- Procédure AGR-P-02 Sécurité des centres d'évaluation – ANSSI.

2.1.3. Principaux textes réglementaires

- Règlement (UE) 2019/881 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité) ;
- Règlement d'exécution (UE) 2024/482 de la Commission du 31 janvier 2024 portant modalités d'application du règlement (UE) 2019/881 du Parlement européen et du Conseil en ce qui concerne l'adoption du schéma européen de certification de cybersécurité fondé sur des critères communs (EUCC) ;
- Instruction interministérielle n° 901/SGDSN/ANSSI du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles ;
- Instruction interministérielle n° 300/SGDSN/ANSSI du 23 juin 2014 relative à la protection contre les signaux parasites compromettants – Annexe 2 ;
- Document relatif à l'accréditation harmonisée des organismes d'évaluation de la conformité : « Accreditation of ITSEFs for the EUCC ».

2.1.4. Guides et normes techniques d'application recommandée

- Guide d'homologation de sécurité – ANSSI ;
- Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte – ANSSI ;
- ISO/IEC 19896 : Techniques de sécurité IT – Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information - Partie 1 : Introduction, concepts et exigences générales
- ISO/IEC 19896 : Techniques de sécurité IT – Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information - Partie 3 : Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408.

2.2. Abréviations et définitions

Pour les besoins du présent document, les termes et définitions ci-après s'appliquent :

- **Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)** : autorité nationale de certification de cybersécurité (ANCC) au sens du Règlement UE 2019/881 ; Centre de certification pour la sécurité offerte par les technologies de l'information au sens de l'article 56.6 du même règlement.
- **Centre d'évaluation de la sécurité des technologies de l'information (CESTI)** : laboratoire réalisant les activités d'évaluation spécifiées dans les Critères communs, en sous-traitance d'un organisme certificateur, accrédité selon les référentiels NF EN ISO/IEC 17025 et ISO/IEC TS 23532 ainsi que les documents Cofrac associés.
- **Cible de sécurité** : exigences que doivent respecter les produits ou les sites évalués et leur documentation associée.
- **Critères d'évaluation** : normes ou spécifications énonçant les règles de définition des exigences de sécurité et les méthodes d'évaluation du respect de ces exigences.
- **Fournitures** : produit(s) de sécurité et documentation associée soumis à l'évaluation de la conformité.
- **Organisme certificateur (OC)** : organisme accrédité selon la norme ISO/IEC 17065, et, le cas échéant, autorisé pour la délivrance de certificats EUCC au sens du CSA et de l'acte d'exécution 2024/482 ; l'ANSSI est instituée par la loi Cyber centre de certification au sens de l'article 56.6 du CSA (certificats de niveau d'assurance « Elevé »).

Il convient de lire dans la norme NF EN ISO/IEC 17025 :

- **Client** : commanditaire de l'évaluation. Le commanditaire peut être le développeur du produit et de sa documentation associée.
- **Données d'essai** : résultats et conclusions des travaux d'évaluation.
- **Enregistrements** : éléments de preuve d'application des procédures et des méthodes.
- **Essai** : évaluation.
- **Laboratoire d'essais** : CESTI Centre d'Evaluation de la Sécurité des Technologies de l'Information.
- **Méthode d'essai** : méthode d'évaluation à laquelle sont associés des critères d'évaluation.
- **Objets soumis à essai** : fournitures (produit et sa documentation d'évaluation).
- **Rapport d'essai** : Rapport Technique d'Evaluation final, partiel ou pour composition (RTE).

Sigles :

- **ANCC** : Autorité Nationale de Certification de Cybersécurité (National Cybersecurity Certification Authority)
- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information
- **CC** : (Common Criteria) Critères Communs d'évaluation de la sécurité des technologies de l'information
- **CEM** : (Common Evaluation Methodology) Méthodologie commune d'évaluation de la sécurité des technologies de l'information
- **CESTI** : Centre d'Evaluation de la Sécurité des Technologies de l'Information
- **CSA :** Cybersecurity Act
- **ENISA** : Agence européenne chargée de la sécurité des réseaux et de l'information (European Union Agency for Cybersecurity)
- **EA :** European co-operation for Accreditation

- **EUCC** : Schéma européen de certification de cybersécurité basé sur les critères communs (Common Criteria based European candidate Cybersecurity Certification scheme)
- **OC** : Organisme Certificateur
- **RTE** : Rapport Technique d'Evaluation
- **TIC** : Technologie de l'Information et de la Communication

3. DOMAINE D'APPLICATION

Le champ d'application du présent document d'exigences spécifiques concerne les exigences à mettre en œuvre par les laboratoires dans le cadre de l'évaluation de la sécurité des technologies de l'information selon le schéma EUCC et conformément au CSA, comme décrit en objet de ce document.

L'évaluation de la sécurité d'un produit des technologies de l'information selon les Critères Communs consiste à vérifier que ce produit est conforme aux spécifications de sécurité décrites dans un document intitulé « cible de sécurité ». Ces spécifications sont énoncées conformément à un référentiel normalisé (norme ISO/IEC 15408). La conformité du produit à ces spécifications est évaluée selon la méthodologie associée CEM (norme ISO/IEC 18045).

La certification d'un produit est prononcée par un organisme certificateur accrédité et notifié par l'ANSSI auprès de la Commission européenne. Le schéma de certification EUCC prévoit l'émission de certificats correspondant aux niveaux d'assurance « Substantiel » et « Elevé » au sens du CSA.

La certification se base sur l'évaluation de la sécurité de ce produit par un laboratoire accrédité et notifié par l'ANSSI auprès de la Commission européenne. L'accréditation par le Cofrac suivant ce document d'exigences spécifiques est donc un pré requis à la réalisation d'évaluations pour le compte d'un organisme certificateur accrédité, et le cas échéant, autorisé à délivrer un certificat EUCC.

Lorsqu'un laboratoire vise à réaliser des évaluations en vue de la certification d'un produit au niveau « Substantiel », il doit faire l'objet d'une accréditation selon le présent document pour les tests concernés. Lorsqu'il vise à réaliser des évaluations en vue de la certification d'un produit au niveau « Elevé », il doit en plus faire l'objet d'une autorisation par l'ANSSI.

Ce document s'adresse aux :

- CESTI accrédités et notifiés ou candidats à l'accréditation et à la notification en vue de réaliser des évaluations de produits au profit d'un organisme certificateur accrédité et notifié ou candidat à l'accréditation et à la notification conformément aux règlements (UE) 2019/881 et (UE) 2024/482
- évaluateurs du Cofrac pour lesquels il constitue une base d'harmonisation pour l'évaluation ;
- membres des instances décisionnelles du Cofrac (Comité de Section, Commission d'Accréditation concernée par ce domaine), pour lesquels il constitue un outil d'aide à la décision ;
- membres de la structure permanente du Cofrac ;
- clients des laboratoires d'essais accrédités sur ce domaine ;
- instances officielles concernées par ce domaine ;
- organismes certificateurs.

4. MODALITES D'APPLICATION

Ce document est applicable à compter du **01 mai 2024**.

Dans ce document, les formes verbales suivantes sont utilisées.

Le terme « **doit** » exprime une exigence. Les exigences correspondent à la retranscription des exigences de la norme d'accréditation, du prescripteur ou de la réglementation, ou relèvent des règles d'évaluation et d'accréditation du Cofrac.

Le terme « **devrait** » exprime une recommandation de bonne pratique. L'organisme est libre de ne pas suivre la recommandation s'il peut démontrer que les dispositions alternatives qu'il met en œuvre satisfont les exigences d'accréditation.

Le terme « **peut** » exprime une permission ou une possibilité. La possibilité est généralement employée pour indiquer des moyens de satisfaire une exigence donnée, que l'organisme est libre d'appliquer ou non.

5. MODIFICATIONS APPORTEES A L'EDITION PRECEDENTE

Il s'agit de l'édition initiale du document.

6. DEFINITION DE LA PORTEE D'ACCREDITATION

Le laboratoire candidat au titre du présent document peut demander à être accrédité pour évaluer les types de produits et les sites suivants :

- Logiciels et équipements réseau
- Composants électroniques, microélectroniques et leurs logiciels embarqués[2]
- Equipements matériels avec boîtiers sécurisés
- Sites de développement ou de fabrication

Les sites de développement objets de la portée d'accréditation sont uniquement ceux correspondant aux types de produits couverts.

La nomenclature du domaine est disponible dans le document LAB INF 34.

7. EXIGENCES POUR LES LABORATOIRES

Dans le cadre de sa démarche d'accréditation, du maintien et du renouvellement de cette dernière, le CESTI doit satisfaire aux exigences générales du Cofrac, aux exigences des méthodes d'essais, aux exigences portées par les documents listés aux § 2.1.1, 2.1.2, 2.1.3, ainsi qu'aux exigences spécifiques contenues dans le présent document, développées ci-après.

Le tableau ci-dessous constitue une aide à la compréhension de l'interaction des différentes exigences applicables.

[2] Ces types de produits font l'objet de domaines techniques dédiés dans le schéma EUCC, associés à des référentiels et méthodes d'attaque spécifiques permettant l'émission de certificats EUCC jusqu'au niveau EAL 7 des Critères communs.

NF EN ISO/IEC 17025	Annexe au règlement (UE) 2019/881*	Accreditation of ITSEFs for the EUCC	ISO/IEC TS 23532-1
§ 4 Impartialité, Confidentialité	2 à 8, 13, 14, 16, 17	§ 6.2.1[3] § 6.2.2	§ 4.2.6 § 4.2.8
§ 5 Exigences structurelles	1	/	§ 5.3.1
§ 6.1 Exigences relatives aux ressources - Généralités	11	/	/
§ 6.2 Personnel	8, 10 et 12	§ 6.2.3	§ 6.2
§ 6.3 Installations et conditions ambiantes	11	/	/
§ 6.4 Equipements	11	/	§ 6.4
§ 6.6 Produits et services fournis par des prestataires externes	7, 9 et 20	§ 6.2.4 § 6.2.5	/
§ 7.1 Revue des demandes, appels d'offres et contrats	18	/	/
§ 7.2 Sélection, vérification et validation des méthodes	10	/	/
§ 7.5 Enregistrements techniques et §8.4 Maitrise des enregistrements	/	§ 6.2.7	/
§ 7.7 Assurer la validité des résultats et § 7.10 Travaux non conformes	/	§ 6.2.6 § 6.2.8	/
§ 7.8 Rapport sur les résultats		/	§ 6.5 § 7.8
§ 8.2 Documentation du système de management	/	§ 6.2.9	/
§ 8.8 Audit interne	/	§ 6.2.10	/

* les exigences 15 et 19 ne rentrent pas dans le périmètre d'évaluation des évaluateurs.

Des exigences additionnelles à la norme NF EN ISO/IEC 17025 sont décrites dans le document Accreditation of ITSEFs for the EUCC concernant :

- L'évaluation en composition (cf. Partie 1 chapitre 14 des Critères Communs) – les exigences à respecter étant décrites au § 6.2.11 ;

Pour cette exigence et dans le cas où un CESTI demande une accréditation pour la réalisation d'évaluation en composition pour d'autres méthodes que celles harmonisées, celui-ci en informe le Cofrac et l'OC afin d'examiner la faisabilité de la demande.

[3] Le document EA 2/20 définit l'approche d'EA pour évaluer l'indépendance des organismes d'évaluation de la conformité (OEC) et des activités d'évaluation de la conformité (tierce partie) de ces OEC réalisées à des fins de notification. Ce dernier est disponible en version Française au lien suivant : https://tools.cofrac.fr/documentation/EA-2-20-G. Certains cas présentés sont susceptibles de ne pas s'appliquer aux laboratoires accrédités selon le référentiel NF EN ISO/IEC 17025 : 2017.

- La surveillance des vulnérabilité - les exigences à respecter étant décrites aux § 6.2.13 et § 6.2.13.

Pour cette exigence, le CESTI peut avoir une procédure de surveillance des vulnérabilités des produits qu'il a évalués. Celle-ci devrait inclure la gestion des vulnérabilités portées à sa connaissance et les actions à mettre en place après la détection d'une vulnérabilité (comment remonter l'information et à qui, …).

Cette exigence n'implique pas de retester systématiquement le produit ou d'avoir mis en œuvre un système de surveillance pour toute vulnérabilité.

7.1. Exigences structurelles

NF EN ISO/IEC 17025:2017 (LAB REF 02), § 5.3
ISO/IEC TS 23532:2021, § 5.3.1

L'organisation du CESTI doit respecter les exigences de sécurité telles que décrites dans l'annexe B du présent document.

7.2. Personnel

NF EN ISO/IEC 17025 :2017 (LAB REF 02), § 6.2
ISO/IEC TS 23532:2021, § 6.2

Le CESTI doit attribuer des rôles tels que définis dans la norme ISO/IEC TS 23532 :2021 § 6.2. Pour cela, le CESTI définit des critères d'habilitation objectifs qui devraient suivre les recommandations exposées en annexe A du présent document.

Le CESTI gère les compétences techniques de ses personnels en se basant sur la nomenclature définie dans le document LAB INF 34, et devrait, pour les compétences d'évaluation des « Critères communs », s'appuyer sur la norme ISO/IEC 19896-3.

7.3. Installations et conditions ambiantes

NF EN ISO/IEC 17025 :2017 (LAB REF 02), § 6.3

Le CESTI doit disposer de locaux, de moyens et d'accès adaptés aux activités d'évaluation (bureaux, plate-forme de tests, salle de réunion…) qui doivent être protégés contre les agressions et intrusions, notamment celles résultant d'actes frauduleux ou malveillants.

Pour ce faire, le CESTI doit respecter les exigences de sécurité telles que décrites dans l'annexe B du présent document.

7.4. Equipements

NF EN ISO/IEC 17025:2017 (LAB REF 02), § 6.4
ISO/IEC TS 23532:2021, § 6.4

Le CESTI doit disposer dans la mesure du possible de ses propres moyens de test. Les critères d'évaluation prévoient que les CESTI puissent ne pas disposer de tous les équipements de test, en particulier, lorsqu'il s'agit de logiciels ou équipements spécifiques. Dans le cas où le CESTI est obligé d'utiliser un équipement qu'il ne maitrise pas en permanence, la qualité, l'intégrité et la sécurité de l'équipement doivent être assurées. Le CESTI doit également s'assurer que l'utilisation de cet équipement ne remet pas en cause la confidentialité des informations associées au produit ou de ses propres procédures d'évaluation. Il doit avoir accès aux outils de test du développeur. Une partie de l'évaluation peut alors être effectuée sur le site fournisseur, mais cette situation doit toutefois rester exceptionnelle.

Lorsqu'un équipement informatique est utilisé pour effectuer une évaluation, la configuration de cet équipement au moment de l'évaluation doit être établie, tracée et conservée. La configuration doit lister la version des différents logiciels et outils utilisés pour l'évaluation.

Le CESTI doit être en mesure d'apporter la preuve que les outils logiciels et équipements qu'il met en œuvre réalisent la fonction attendue, et qu'ils n'interfèrent pas dans la réalisation des tests.

7.5. Produits et services fournis par des prestataires externes

NF EN ISO/IEC 17025:2017 (LAB REF 02), § 6.6

Le recours à la sous-traitance d'activités d'évaluation est soumis à l'acceptation préalable de l'organisme certificateur ainsi qu'à celle du commanditaire et du développeur concernés. En complément, le CESTI ne peut sous-traiter des activités qu'à un laboratoire accrédité et notifié.

Dans le cadre de prestations conjointes sur la partie matérielle et logicielle des évaluations d'équipements avec boitier sécurisé, les deux CESTI doivent être accrédités et notifiés.

7.6. Sélection, vérification et validation des méthodes

NF EN ISO/IEC 17025:2017 (LAB REF 02), § 7.2
LAB REF 08

Les méthodes d'essais utilisées par le CESTI résultent de l'application de méthodes normalisées, d'une adaptation de méthodes normalisées ou reconnue, ou d'un développement spécifique.

Le CESTI doit valider les méthodes d'essai qu'il a adaptées ou développées afin de confirmer qu'elles sont aptes à l'emploi prévu. La validation de ces méthodes se fait dans le cadre de projets pilotes.

8. MODALITES D'EVALUATION DES LABORATOIRES

Compte tenu des exigences réglementaires auxquelles doit répondre le CESTI pour assurer la sécurité physique et logique, le Cofrac peut être amené à augmenter la durée des évaluations des laboratoires, par rapport aux durées préconisées dans le document Cofrac LAB REF 05.

Lorsque la portée d'accréditation du laboratoire le nécessite, le Cofrac peut être amené à mandater un (ou plusieurs) évaluateur(s) technique(s) Cofrac supplémentaire(s) en fonction de l'étendue des compétences techniques revendiquées

En particulier, l'équipe d'évaluation doit comporter au moins un évaluateur Cofrac maîtrisant les Critères Communs, et un évaluateur maîtrisant une (ou plusieurs) compétence(s) technique(s) identifiée(s) dans le LAB INF 34 et revendiquée(s) par le CESTI.

Les exigences de l'annexe B font l'objet d'une évaluation spécifique par un évaluateur Cofrac sur une journée dédiée dans le cadre de l'évaluation initiale.

Puis, ces exigences sont réévaluées au moins une fois dans le cycle d'accréditation sur une demi-journée dédiée, en fonction des modifications apportées à la politique de sécurité ou à l'architecture du système informatique (SI).

L'organisme certificateur pour le compte duquel le CESTI réalise des prestations (évaluations) informe le Cofrac et le CESTI concerné des manquements qu'il identifie dans le cadre du suivi des évaluations qu'il réalise. Le Cofrac examine la situation relevée et peut déclencher, le cas échéant, une évaluation supplémentaire.

Le Cofrac informe l'ANSSI du résultat des évaluations lorsqu'un changement dans le statut de l'accréditation intervient (non-renouvellement, suspension, retrait ou résiliation totale ou partielle de l'accréditation…) et, dans tous les cas, transmet un exemplaire du rapport d'évaluation des CESTI à l'ANSSI.

Annexe A (informative) – Compétences techniques des laboratoires

Gestion des compétences (internes du personnel du laboratoire)

La norme ISO 19896-1 définit au chapitre 6 des niveaux de compétences Niveau 1 à Niveau 4. Ces niveaux sont définis de manière globale et ne peuvent être directement ramenés à une compétence ou une technique particulière (cf. Niveau 2 : « *Is competent to work unsupervised in many testing or evaluation areas but can require supervision in a few areas* »).

Les niveaux atomiques suivants devraient être utilisés pour le suivi et l'évaluation des compétences du personnel des CESTI relatives aux différentes méthodes et techniques de leur portée d'accréditation.

	Niveaux de compétence atomique	Définition
C	Connaissance	Est capable de réaliser des tests ou activités d'évaluation relevant de cette méthode ou technologie particulière sous la supervision d'un expert.
M	Maîtrise	Est capable de travailler de façon autonome sur cette méthode ou technologie particulière.
E	Expertise	Est capable de travailler de façon autonome sur cette méthode ou technologie particulière ; est en mesure d'assurer la supervision ou la revue des travaux réalisés par un évaluateur CESTI de niveau C ou M sur cette méthode ou technologie particulière.

Niveaux de compétence globaux issus de l'ISO 19896-1	Relation avec les niveaux de compétence 'atomique'
Niveau 1	Un évaluateur CESTI qualifié 'Niveau 1' sera positionné au niveau de compétence 'C' sur une majorité des éléments de la portée d'accréditation du laboratoire.
Niveau 2	Un évaluateur CESTI qualifié 'Niveau 2' sera positionné au niveau de compétence au moins 'M' sur une majorité des éléments de la portée d'accréditation du laboratoire.
Niveau 3	Un évaluateur CESTI qualifié 'Niveau 3' sera positionné au niveau de compétence au moins 'M' sur une majorité des éléments de la portée d'accréditation du laboratoire et au niveau 'E' sur un sous ensemble significatif des éléments de la portée au regard de l'activité du CESTI.
Niveau 4	Le passage du 'Niveau 3 ' au 'Niveau 4' s'apprécie au regard d'autres compétences (gestion de projet, compétences managériales) et de l'expérience de l'évaluateur dans la réalisation d'évaluations Critères communs.

La qualification formelle des évaluateurs selon la taxonomie définie au Chapitre 6 de l'ISO 19896-1 n'est pas requise. Toutefois, l'attribution des rôles de responsable technique du laboratoire (Niveau 4), responsable d'évaluation CESTI (Niveau 3 ou 4) ou valideur/signataire des RTE (Niveau 4) devrait tenir compte des critères relevant du niveau correspondant.

Annexe B (obligatoire) – Exigences de sécurité relatives à la protection physique et logique du laboratoire

a) Le CESTI doit protéger au minimum au niveau Diffusion restreinte [instructions interministérielles relatives à la protection des systèmes d'informations sensibles n° 901/SGDSN/ANSSI] les informations sensibles relatives à la prestation et notamment les documents transmis par le commanditaire, les informations collectées dont le code source et les informations de conception, et les rapports d'évaluation.

b) Le CESTI doit respecter les règles établies dans les instructions interministérielles relatives à la protection des systèmes d'informations sensibles (n° 901/SGDSN/ANSSI) et à la protection contre les signaux parasites compromettants (n° 300/SGDSN/ANSSI – Annexe 2). Le CESTI devrait s'appuyer notamment sur le guide « Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte » de l'ANSSI.

c) Le CESTI doit homologuer son système d'information au niveau Diffusion Restreinte. Le CESTI devrait pour cela utiliser le Guide d'homologation de sécurité de l'ANSSI.

d) Le CESTI doit identifier et mettre en œuvre les exigences du document AGR-P-02 qui lui sont applicables au regard de son activité et doit justifier les exigences non appliquées.